通信システムの検証に関する研究

氏名	神長裕明（かみながひろあき）
授与学位	工学博士
学位授与年月日	平成元年3月24日
学位授与の根拠法規	学位規則第5条第1項
研究科，専攻の名称	東北大学大学院工学研究科 （博士課程）情報工学専攻
学位論文題目	**通信システムの検証に関する研究**
指導教官	東北大学教授 野口 正一
論文審査委員	東北大学教授 野口 正一　東北大学教授 城戸 健一 東北大学教授 木村 正行　東北大学助教授 白鳥 則郎

論文内容要旨

情報通信システムの普及発展に伴い，ネットワークアーキテクチャを標準的に定めることが必須となっており，ネットワークアーキテクチャの規定を正確かつ厳密に行うためにＦＤＴ（Formal Description Technique）と呼ばれる，形式的記述法が開発されている。アーキテクチャの仕様を形式的に記述することは，仕様の意味を明確にするだけでなく，検証に対する形式的な枠組みを与え，検証の自動化への道を開くものである。ＩＳＯおよびＣＣＩＴＴが現在研究を進めているＦＤＴとして，拡張状態遷移機械モデルに基づいたＳＤＬおよびEstelleと，抽象的な概念に基づいたＬＯＴＯＳがある。ＬＯＴＯＳ（Language Of Temporal Ordering Specification）は，ＩＳＯで開発されたイベントの時間順序の概念に基づいたＦＤＴであり，ネットワークアーキテクチャにおける階層のサービス定義とプロトコル仕様の記述や，両者の間の無矛盾性の検証に適している。サービス定義とプロトコル仕様の間の無矛盾性の検証は，通信システムにおける主要な検証問題の一つである。これを形式的に行う方法としては，代数的仕様記述法に基づいたＡＦＦＩＲＭテステムがあり，検証は一方の仕様から他方の仕様の性質を示す問題に帰着する。一方，ＬＯＴＯＳにおいては，二つの仕様の等価性を示す問題である。ＬＯＴＯＳに関するこれまでの研究として，トランスポート層のＬＯＴＯＳによる記述や，サービス定義とプロトコル仕様の間の等価性を代数的な規則のみを用いて変換し，一致することを示した例などが報告されている。しかし，任意の二つのＬＯＴＯＳ仕様の等価性を代数的な規則のみを用いて示すことは，代数的な規則の不完全性や規則の適用の仕方の問題により，一般に決定不能であり，ＬＯＴＯＳ仕様の等価性を判定するための方法論

の開発が急務となっている。本論文は，この立場に立って，ＬＯＴＯＳで記述された二つのシステム（例えば，サービス定義とプロトコル仕様）の間の等価性を検証するための方法論を研究したもので，全編７章より成る。

第１章は，序論で，本論文の背景について述べている。

第２章では，本論文の対象であるＬＯＴＯＳについて，その概要，シンタックス，セマンティックス，ＬＯＴＯＳ仕様の形式的モデルであるＬＴＳ（Labelled Transition System）およびＩＳＯで定義した弱 bisimulation 等価性の定義について述べている。

第３章では，ＬＯＴＯＳ仕様の等価性のＩＳＯ定義である弱 bisimulation 等価性に対して，ｋ－弱 bisimulation 等価性および準強 bisimulation 等価性という二つの新しい等価性の概念を導入し，弱 bisimulation 等価性との関係について考察している。ｋ－弱 bisimulation 等価性は，すべての長さのイベントについて考慮しなければならない弱 bisimulation 等価性に比べて，長さがｋ以下の観測可能なイベントのみを扱えばよいという点において，弱 bisimulation 等価性よりも定義が簡単であり，従って，等価性の判定がし易いという利点がある。ＬＯＴＯＳ仕様の形式的モデルであるＬＴＳに対して，二つのＬＴＳが弱 bisimulation 等価であることとｋ－弱 bisimulation 等価であることが，互いに必要かつ十分な条件になることが示され，ｋ－弱 bisimulation 等価性の定義に基づいて弱 bisimulation 等価性の判定が容易に行えることが示されている。同時にｋの値は１でもよいことが示されている。併せて，ＬＴＳが有限である場合（ＦＴＳ）に対して，１－弱 bisimulation 等価性を判定するために，標準的な１－弱 bisimulation 関係を与え，この標準的な１－弱 bisimulation 関係に基づいて，１－弱 bisimulation 等価性の判定が手続的に行えることを示している。また，準強 bisimulation 等価性は，内部イベントもふくめてただ１つのイベントによる遷移のみを扱えばよいという点において，１－弱 bisimulation 等価性よりも定義が簡単であり，等価性の判定がさらにし易いという利点がある。しかし，準強 bisimulation 等価性は１－弱 bisimulation 等価性よりも強い等価性であり，二つのＬＴＳが準強 bisimulation 等価であることと１－弱 bisimulation 等価であることは，互いに必要かつ十分な条件とはならない。そこで，二つのＬＴＳ Sys 1 と Sys 2 をその推移的閉包 Sys 1 ' と Sys 2 'に変換し，Sys 1 と Sys 2 が１－弱 bisimulation 等価であることと Sys 1 ' と Sys 2 'が準強 bisimulation 等価であることが互いに必要かつ十分な条件になることを示し，準強 bisimulation 等価性を用いて１－弱 bisimulation 等価性すなわち弱 bisimulation 等価性の判定が容易に行えることを示している。併せて，ＦＴＳに対して，１－弱 bisimulation 等価の場合と同様に，標準的な準強 bisimulation 関係を与え，この標準的な準強 bisimulation 関係に基づいて，準強 bisimulation 等価性の判定が手続的に行えることを示している。

第４章では，まず，ＬＯＴＯＳ仕様からそのモデルであるＬＴＳを，ＬＯＴＯＳのオペレーショナルーセマンティクスに基づいて，効果的に生成する方法を与えている。ＬＴＳの生成の過程において，弱 bisimulation 合同なＬＯＴＯＳの動作式を，書き換え規則として適用することによって，生成するＬＴＳの状態数の減少が図られている。次に，有限オートマトンにおける等価な状態の同値類分割と同様な概念に基づいて，“有限”の状態を持つ二つのＬＯＴＯＳ仕様の弱 bisimulation

等価性を判定するための，具体的な興味深いアルゴリズムを与えている。

第５章では，ＦＴＳに対してその最簡形という，弱 bisimulation 等価性を保存し状態と遷移の数が最少であるＦＴＳの概念を導入し，最簡形と弱 bisimulation 等価性との関係について考察している。二つのＦＴＳが弱 bisimulation 等価であることと，二つのＦＴＳの最簡形が同型になることが互いに必要かつ十分な条件になることが示されている。この性質を用いて，二つのＦＴＳの弱 bisimulation 等価性を判定するときに，各々を最簡形に変換し，その同型性を調べることによって，二つのＦＴＳの等価性を直接判定するよりも，効率よく判定できることを示している。併せて，準強 bisimulation 等価性に基づいた最簡形への変換の方法を与えている。

第６章では，第４章および第５章で提案した等価性の判定法に基づいて，ＬＯＴＯＳ仕様の検証システムの設計を与えている。検証システムは，（１）仕様解析機構，（２）ＦＴＳ生成機構，（３）最簡形変換機構，（４）同型性判定機構，の４つの構成要素から成り立っている。入力として与えられた二つのＬＯＴＯＳ仕様は，まず，仕様解析機構によりシンタックスチェックと静的意味エラーのチェックが行われ，エラーが無ければ中間表現として出力される。二つの中間表現はＦＴＳ生成機構によって，それぞれＦＴＳに変換される。生成されたＦＴＳは，最簡形変換機構によってそれぞれ最簡形に変換され，最後に同型性判定機構によりその同型性が判定され，同型であれば弱 bisimulation 等価であり，同型でなければ弱 bisimulation 等価ではないと結論される。

第７章は，本論文の結論である。

以上本論文は，ＬＯＴＯＳの等価性に関する諸性質を明らかにし，それらの性質に基づいて，有限の状態をもつ任意の二つのＬＯＴＯＳ仕様の間の等価性を手続的（アルゴリズム的）に効率よく判定するための方法論を開発したものである。本論文で提案した判定法は，有限の状態をもつシステムに対しては，必ず適用可能であるという有効性をもっている。

審 査 結 果 の 要 旨

通信システムの形式的な仕様化およびその検証問題に対する研究は，高信頼度の計算機ネットワークを構築する上で極めて重要な問題である。著者は，この立場に立って，通信システム向きの形式的な記述言語であるＬＯＴＯＳで記述された，二つのシステムの間の等価性を検証するための方法を論じ，これを用いて通信システムの検証について研究した。本論文は，その結果をまとめたもので，全編７章より成る。

第１章は序論である。第２章では，本論文の対象であるＬＯＴＯＳの概要およびＩＳＯで定義した弱 bisimulation 等価性の定義について述べている。

第３章では，ｋ－弱 bisimulation 等価性および準強 bisimulation 等価性という二つの新しい等価性の概念を導入し，弱 bisimulation 等価性との関係について考察している。まず，観測可能なイベント系列の長さをｋ以下に制限したｋ－弱 bisimulation 等価性から，二つのＬＯＴＯＳ仕様の弱 bisimulation 等価性が容易に判定できることを示し，同時にｋの値は１でもよいことが示されている。また，ＬＯＴＯＳ仕様を Labelled Transition System（ＬＴＳ）の推移的閉包に変換することによって，本論文で導入した準強 bisimulation 等価性を用いて，二つのＬＯＴＯＳ仕様の弱 bisimulation 等価性が容易に判定できることを示している。さらに，ＬＴＳが有限である場合（ＦＴＳ）については，１－弱 bisimulation 等価性および準強 bisimulation 等価性を判定する基本的な手続を与えている。これらは，重要な結果である。

第４章では，まず，ＬＯＴＯＳ仕様からそのモデルであるＬＴＳを効果的に生成する方法を与え，ついで，二つのＦＴＳの弱 bisimulation 等価性を判定するための簡明なアルゴリズムを与えている。

第５章では，まずＦＴＳに対して，弱 bisimulation 等価性を保存し，状態と遷移の数が最少であるＦＴＳの最簡形の概念を導入している。ついで，最簡形への変換の方法を与え，最簡形へ変換することによって，もとの二つのＦＴＳの等価性を直接判定するよりも効率よく判定できることを示している。これらは，興味ある結果である。

第６章では，第４章および第５章で提案した等価性の判定法に基づいて，ＬＯＴＯＳ仕様の検証システムの設計を与えている。

第７章は，結論である。

以上要するに本論文は，通信システムの設計における基本的な問題である，二つの仕様の間の検証について詳細な研究を行い，検証システム作成のための基礎を与えたもので，通信工学ならびに計算機工学の発展に寄与するところが少なくない。

よって，本論文は工学博士の学位論文として合格と認める。